Georgia Department of Human Resources
Office of Information Technology
Information Security Program: Overview and Strategy

Background and Importance of Information Protection

To fulfill its mission, DHR must collect and use information from a variety of sources, including constituents, employees, partner agencies of government, vendors and other service partners. These information assets are vital to DHR's ability to render human services to the citizens of Georgia and to partner agencies. Failure to protect the integrity and availability of information assets can impair DHR's service delivery capabilities. Further, breeches in personal and federally regulated confidential information can potentially cause personal damage to those individuals impacted by the loss of personal information.

Therefore, the appropriate, lawful protection and use of information assets is critically important to achieving DHR's mission and to maintaining the confidence of the State's constituents. Therefore, all reasonable and lawful measures will be undertaken to ensure that a framework of policies, standards, practices and procedures are in place to support appropriate use and protection of all DHR information assets.

Information Security and Principles of Information Protection

Overall, DHR's Principles of Information Protection rest on the foundation of information security. Data must be secured so that it is available, has integrity, and so that it is protected from unauthorized disclosure. Availability is the umbrella, which gives DHR the obligation and authority to ensure that the data is physically available through the infrastructure—workstations, servers, routers, etc. are protected physically and through personnel and business processes to ensure that business information is available. Then, integrity is the quality that ensures that the data that is accessed is the actual business data—it has not been purposely or inadvertently corrupted or altered. Finally, information assets must be protected so that they are available only to those parties authorized to use or view them. For DHR, this element of information security means to appropriately and legally secure all data while appropriately balancing the requirements of the Georgia Open Records Act, federal HIPAA regulations, and other pertinent legal mandates.

DHR's Principles of Information Protection

DHR's information assets:

1. Will be collected, processed, used and protected fairly and in compliance with the *Georgia Open Records Act*, other applicable laws and guidelines of the State of Georgia, and applicable Federal laws and guidelines.
2. Will be collected, processed, and used only for one or more specified and lawful purposes, and shall not be further transmitted in any manner incompatible with

that purpose or those purposes;
3. Will be adequate, relevant and not excessive in relation to the purpose or purposes for which the information is collected and used;
4. Will be accurate and, where necessary, kept up to date;
5. Will not be kept for longer than is necessary for the specified purpose(s) and properly disposed;
6. Will be collected, processed, and used in accordance with the rights of the constituent and requirements of the data-owner, in accordance with the laws and guidelines of the State of Georgia and the federal government, where applicable.
7. Will be protected under DHR's direct authority. Information assets are subject to appropriate technical and administrative processes to prevent unauthorized or unlawful processing, accidental loss, destruction, or damage to any information asset for which DHR is custodian.
8. Will not be transferred to any jurisdiction, organization, or person outside of DHR that does not uphold the same level of protection for DHR's information asset

Information Security and Strategy for Information Protection

Fulfilling DHR's mission depends upon secure, integrated access to integrated information. Therefore, information security must be operationalized across the enterprise, as a core, internal line of business, or service. A comprehensive, integrated information security program will ensure:

- Higher personalization in delivery of human services
- Alignment with Federal Healthcare Architecture and funding sources
- Operational alignment: lower development costs
- Physical security of assets
- No fines and legal liabilities for lack of compliance or breach of constituent data

The Enterprise Security Framework will be aligned around three primary facets critical for protecting DHR's information assets. These are:

Administrative Safeguards, Physical Safeguards, and **Technical Safeguards**. *Administrative safeguards* are the administrative actions, best practices and procedures to manage the selection, development, implementation of and security measures to protect DHR information assets and to manage the conduct of the DHR workforce in relation to the protection of the information assets. *Physical safeguards* are the physical measures, best practices, and procedures to protect DHR's information assets and related buildings and equipment, from natural and environmental hazards, and from unauthorized intrusion. *Technical safeguards* encompass technology and the best practices and procedures for its use that protect DHR's information assets and control

access to them.

Standards will fall under each of these three safeguard areas and will contain a list of basic procedures, which must be addressed for each DHR line of business to ensure the security of all information assets. Thus, an awareness of business architecture (i.e. DHR lines of business) holds critical importance.

Best Practices and Procedures within the standards will be developed, established, and enforced through a governance committee, the Enterprise Security Steering Committee, which will include representation from all DHR departments and divisions and be closely aligned with the legal and human resources units.

Summary and Conclusion

Information security must be viewed as an enterprise service—vital and critical to preserving the integrity, availability, and authorized access to DHR's information assets. Information security must be operationalized as a joint responsibility of all DHR employees and partners—security is not ensured merely by employing technologies. Rather, all aspects of the administrative, physical and technical safeguards must be appropriately addressed for each DHR line of business. Therefore, the Information Security Officer will work with OIT to use the described enterprise security policy framework and DHR's business architecture to operationalize a comprehensive, effective, information security program.